Timo Ojala

3G-KORTIN HALLINTATYÖKALU

Tietotekniikan koulutusohjelma

Tietoliikennetekniikan suuntautumisvaihtoehto

2009

samk
Satakunnan ammattikorkeakoulu

3G-KORTIN HALLINTATYÖKALU

Ojala, Timo
Satakunnan ammattikorkeakoulu
Tekniikka ja merenkulku Pori
Tietotekniikan koulutusohjelma
maaliskuu 2009
Aromaa, Juha
UDK: 621.39
Sivumäärä:31

Asiasanat: toimikortit, matkapuhelinjärjestelmät, lukulaitteet

---

Tämän opinnäytetyön aiheena oli tutkia matkapuhelinverkkojen toimikorttien rakenteita ja niihin sopivia työkaluja. Työssä tutkittiin USIM-kortin rakennetta, toimintaa, autentikointia ja sen eroa SIM-korttiin. Työssä selvitettiin myös Gemalton Card Admin-sovelluksen käyttöä älykorttien kanssa tehtävässä työssä.

Lukulaitteen käyttöä tutkittiin eri älykorttien kanssa, siinä missä se oli mahdollista. Lisäksi luotiin tiivis ohjeistus Card Admin-sovelluksen asennukseen ja käyttöön.

Keskeisimpänä teoriapohjana työssä käytettiin ETSI:n spesifikaatioita ja alan kirjallisuutta.

ADMINISTRATIVE TOOL FOR 3G CARD

Ojala, Timo
Satakunta University of Applied Sciences
Faculty of Technology and Maritime Management Pori
Information technology
April 2009
Aromaa, Juha
UDC: 621.39
Number of Pages: 31

Key Words: smart card, mobile telecommunication systems, card readers

---

The purpose of this thesis was to study the USIM card structure and tools that can be used to do this. This thesis consists of studies of USIM card structure, functions, authentication and its differences compared to SIM-card. Gemalto's Card Admin software's functions to attain this information was also studied in this thesis.

Different available cards were tested with the card reader. This thesis includes compact instructions for using and installing the Card Admin software.

Basis for theory of this thesis were ETSI standards for USIM and SIM card and literature of this field.

SISÄLLYS

LYHENNELUETTELO

2G	Second Generation
3G	Third Generation
3GPP	The 3rd Generation Partnership Project
ADF	Application DF
ADN	Abbreviated Dialling Numbers
AID	Application Identifier
ARR	Access Rule Reference
AUTN	Authentication Token
AV	Authentication Vector
CHV	Cardholder Verification
DF	Dedicated File
ECC	Emergency Call Codes
EDGE	Enhanced Data rates for Global Evolution
EEPROM	Electrically Erasable Programmable Read Only Memory
EF	Elementary File
ETSI	European Telecommunications Standardisation Institute
GSM	Global System for Mobile Communications
HSDPA	High-Speed Downlink Packet Access
IK	Integrity Key
IMSI	International Mobile Subscriber Identity
LND	Last Number Dialed
MAC	Message Authentication Code
MF	Master File
MMS	Multimedia Messaging Service
MMSICP	MMS Issuer Connectivity Parameters
NEPAR	Network Parameters
PIN	Personal Identification Number
PBR	Phone Book Reference file
PSEUDO	Pseudonym
RAM	Random Access Memory
ROM	Read Only Memory

SIM	Subscriber Identity Module
START-HFN	Initialisation values for Hyperframe number
UICC	Universal Integrated Circuit Card
UMTS	Universal Mobile Telecommunications System
USIM	Universal Subscriber Identity Module
UST	USIM Service Table
WLAN	Wireless Local Area Network

1 JOHDANTO

Matkapuhelimien yksinä tärkeimmistä osista ovat jo monia vuosia olleet toimikortit. Nämä kortit ovat mahdollistaneet GSM-teknologian leviämisen yhdeksi käytetyimmistä matkapuhelinteknologioista. Kehityksen edetessä on ollut tarpeen kehittää myös toimikortteja. Toisen sukupolven toimikortin korvaajaksi on noussut kolmannen sukupolven toimikortti.

Tässä opinnäytetyössä selvitetään USIM-kortin toimintaa, niin matkapuhelinverkossa kuin itsenäisesti toimivana matkapuhelimen osana. Aluksi työssä selvennetään lyhyesti älykorttien historiaa, käyttöä tänä päivänä, sekä niiden rakennetta.

Älykorttien perustietojen ollessa lukijalla selvillä, käsitellään työssä SIM- ja USIM-korttien eroja. Suurimpana erona tässä huomataan autentikointi, jonka tietoturvallisuus on huomattavasti parantunut USIM-kortin myötä. Tiedostorakenteessa ja toiminnoissa on myös selkeitä eroja. Korttien yhteensopivuus on kuitenkin myös huomattava.

Tutkimusosassa on käsitelty Gemalton Card Admin-ohjelmaa, lähtien liikkeelle asennuksesta ja edeten lopulta kortin autentikoinnin testaamiseen. Ohjelman perustoiminnot on selvitetty ja niiden tutkimus- ja opetuskäyttöön soveltuvat ominaisuudet esitelty.

2 ÄLYKORTIT

2.1 Historia

Älykortteja on ollut olemassa jo monia vuosia. Nykyään monille tutumpi muoto älykortista on esimerkiksi pankkikorteissa käytettävä älykortti, josta yleisimmin käytetään nimitystä sirukortti. Tämän keksinnön ja älykorttien suosion juuret juontavat jo 1970-luvun Ranskaan. Vuonna 1974 ranskalainen Roland Moreno patentoi ensimmäisen muoviselle kortille asetetun piisirukortin. 1990-luvulla älykortteihin saatiin asennettua ensimmäiset prosessoripiirit. Tätä ennen ne olivat toimineet pääosin muistikortteina. Prosessoripiirien myötä älykorteille aukesi täysin uusia käyttömahdollisuuksia, joista suurimmaksi nousi nopeasti käyttö GSM-puhelimien (Global System for Mobile Communications) SIM-kortteina (Subscriber Identity Module). GSM on toisen sukupolven digitaalinen matkapuhelinjärjestelmä. GSM-puhelimen tärkein osa on SIM-kortti. SIM-kortti on yksi älykorttimalli ja siihen varastoidaan tiedot, joita puhelin tarvitsee toimiakseen matkapuhelinverkossa. /1, 2, 3/

2.2 Nykyhetki

Älykorttien suosio on pääosin niiden tietoturvallisuuden ansiota. Niitä voidaan myös käyttää kannettavien sovellusten alustoina. Tällä hetkellä eri puolilla maailmaa on käytössä yli 2 miljardia älykorttia pelkästään telekommunikaatiolaitteissa. Osa käyttäjistä ei ole ikinä nähnyt tätä korttia, vaikka edustaakin teknologisen kehityksen terävintä kärkeä. /1/

Älykorttien suosiota on lisännyt moni asia. Tietotuvallisuuden lisäksi niiden valmistus on halpaa. Ne ovat pienikokoisia, vievät vähän virtaa ja niiden valmistukseen on olemassa ETSI:n (European Telecommunications Standardisation Institute) määrit-

tämät standardit. ETSI on organisaatio joka tuottaa globaaleja sovellettavia standardeja tietoliikennetekniikan eri aloille. Näissä standardeissa määritellään rajat sille, miten esimerkiksi älykortteja tulee valmistaa ja mitä ominaisuuksia niissä on oltava. /1, 4/

Älykorteilla on tietysti vahvuuksiensa lisäksi myös heikkouksia. Koska niissä ei ole omaa virtalähdettä, eikä käyttöjärjestelmää ne ovat täysin riippuvaisia toisista laitteista. Älykorteille ei ole taattu jatkuvaa virransyöttöä, siksi niihin ole myöskään valmistettu sisäistä kelloa. Tässäkin asiassa älykortit ovat täysin riippuvaisia toisen laitteen kellosta. /1, 2/

2.3 Älykorttien rakenne

Älykortit voidaan jakaa kahdella tavalla. Yksi tapa on jakaa ne muistikortteihin ja prosessorikortteihin. Muistikortissa ei ole prosessoria suorittamaan varsinaisia tehtäviä, kun prosessorikortissa nimensä mukaisesti taas on. Prosessorikortit voidaan jakaa vielä kahteen eri luokkaan, niihin joissa on kryptoprosessori ja niihin joissa sitä ei ole. Kryptoprosessorikortteja käytetään esimerkiksi pankkikorteissa ja SIM-kortteina. /2/

Toinen tapa on jakaa älykortit kontaktillisiin ja kontaktittomiin kortteihin. Kontaktilliset kortit vaativat fyysisen kontaktin toisen laitteen kanssa toimiakseen. Näitä ovat esimerkiksi mobiililaitteissa käytetyt SIM-kortit. Kontaktittomissa korteissa on korttiin liitetty antenni joka toimii välittimenä toisen laitteen ja älykortin välillä. Näitä kortteja käytettään esimerkiksi maksuvälineinä joukkoliikenteessä. /2/

2.3.1 Tiedostorakenne

Älykorttien tiedostorakenteen perustana on ISO 7816-4 standardi. Älykorttien tiedostot jaetaan kolmeen luokkaan. MF (Master File) eli päähakemisto, DF (Dedicated File) eli alihakemisto ja varsinainen tiedosto EF (Elementary File). MF on siis aina lähtökohta eli hierarkian ylin osa, tämän alle sijoittuu sitten joko suoraan DF-alihakemistoja tai EF-tiedostoja. MF-päähakemistossa voi olla monta eri DF-alihakemistoa, ja DF-alihakemistossa voi taas olla toisia DF-alihakemistoja ja EF-tiedostoja. /2/

Jokaiselle tiedostolle on määritelty käyttöoikeudet, joilla hallitaan sitä, kuka tiedostoa saa käsitellä. Käyttöoikeuksia rajoittavat PIN-koodit (Personal Identification Number). PIN-koodi on yleiskäsite yleensä nelinumeroisen numerosarjan kysymiseen. Tietyt oikeudet aukeavat sitten tietyllä PIN-koodilla. Esimerkiksi tiedostoon voi olla lukuoikeudet, mutta tietojen muuttamiseen vaaditaan PIN-koodi. Tiedostoilla voi olla esimerkiksi luku-, kirjoitus-, poisto- tai lukitusrajoituksia. /2/

2.3.2 Älykorttien muistit

Älykortit sisältävät erilaisia muistityyppejä. Perusmuistien ROM (Read Only Memory) lukumuistin, RAM (Random Access Memory) luku- ja kirjoitusmuistin ja EEPROM (Electrically Erasabel Programmable Read Only Memory) sähköisesti ohjelmoitavan ja tyhjennettävän lukumuistin, lisäksi älykorteilla on myös flash-muistia. /2/

RAM-muistia käytetään älykortin työmuistina, johon kortti tallentaa välittömästi käytettävää dataa. RAM-muisti kaikkiin muihin muisteihin nähden eniten fyysistä tilaa kortilta vievä muisti. Tyypillisin RAM-muistin määrä älykortilla on muutamasta kilotavusta kymmeneen kilotavuun. RAM-muistia on pyritty optimoimaan, niin että sitä olisi kortilla juuri sopiva määrä. Mikäli sitä on liian vähän, näkyy se esimerkiksi pitkiä salausalgoritmeja käytettäessä. /2/

ROM-muistiin tallennetaan älykortin valmistusvaiheessa kaikki se tieto, jota ei haluta myöhemmin muutettavaksi. Tällainen voi olla esimerkiksi kortin ydinsovellus. /2/

Älykortin kallein muistityyppi on EEPROM, se määritteleekin usein kortin hinnan. Tälle kortille voidaan tallentaa tietoa useita kertoja, siksi sitä verrataankin usein tietokoneen kovalevyyn. Usein tähän muistiin tallennetaan useita eri sovelluksia. /2/

Flash-muisti on viimevuosien aikana lyönyt itsensä läpi älykorttien muistina ja on osin korvannut ROM-muistin. Flash-muistin etuna on, ettei muistille tallennettavasta koodista tarvitse tehdä erillistä maskia ennen kortin valmistusta. Tämä nopeuttaa kortin valmistamista huomattavasti. /2/

3 SIM (2G) JA USIM (3G)

3G (Third Generation) on kolmannen sukupolven matkapuhelinverkko, jonka standardeja ovat mm. UMTS (Universal Mobile Telecommunications System), joka on Euroopan yleisin 3G-standardi, EDGE (Enhanced Data rates for Global Evolution), joka on alkujaan Amerikassa käyttöönotettu standardi, ns. 2.5G sekä HSDPA (High-Speed Downlink Packet Access), joka on UMTS-pohjainen nopea standardi. 3G-matkapuhelinverkkon myötä, on kehitetty SIM-kortille jatkaja, jonka kapasiteetti ja resurssit takaavat älykorteille tulevaisuuden matkapuhelimien tärkeimpinä osina. /1, 3/

USIM-kortti (Universal Subscriber Identity Module) pystyy toimimaan sekä vanhassa 2G (Second Generation), eli toisen sukupolven matkapuhelinverkkoteknologiassa, että uudemmassa 3G-verkossa. Tämä onkin ollut monille operaattoreille helpotus, koska se mahdollistaa kortin käyttämisen kaikissa heidän verkoissaan, sen tilasta riippumatta. Vaikka SIM-standardit ovat vuodelta 1990 ja USIM-standardit vuodelta 1999, on USIM-kortti vasta nyt saavuttamassa sille varattua paikkaa mobiililaitteiden maailmassa. /1/

3.1 Eroavaisuudet

USIM on päivitetty versio SIM:stä niin tietoturvallisuudessa, tiedon tallentamisessa kuin käyttömahdollisuuksissa. Tärkein ero näiden kahden välillä on se, että SIM-kortti suunniteltiin toimivaksi yhtenä kokonaisuutena, jolloin eroa ohjelmiston ja varsinaisen kortin välillä ei juuri ollut. USIM on käytännössä katsoen ohjelma, jota ajetaan fyysisellä kortilla UICC:lla (Universal Integrated Circuit Card), joka vastaa mobiililaitteen ja USIM-sovelluksen välisestä toiminnasta. USIM-sovellus vastaa verkon autentinkoinnista ja esimerkiksi tekstiviestien varastoinnista. Näin ollen kun puhutaan USIM:sta, tarkoitetaan yleensä koko älykorttia, ei pelkästään USIM-

sovellusta. UICC:lla on mahdollista ajaa samanaikaisesti SIM- ja USIM-sovelluksia, näin voidaan varmistaa kortin toimivuus 2G- ja 3G-verkoissa. /1, 7/

Tärkein ero tietoturvallisuudessa on autentikointi, eli se miten mobiililaite hyväksyy verkon ja miten se hyväksytään verkkoon. USIM:ssa on luonnollisesti myös paljon uusia tiedostoja, joita kaikkia ei 2G-toiminnassa tarvita. Puhelinluetteloa on USIM:ssa paranneltu niin, että siihen voi pelkän nimen ja numeron lisäksi lisätä myös käyttäjän valitsemia muita tietoja. Näitä voivat olla toinen numero, sähköposti- ja katuosoite. /1/

3.1.1 Mobiililaitteen käynnistys

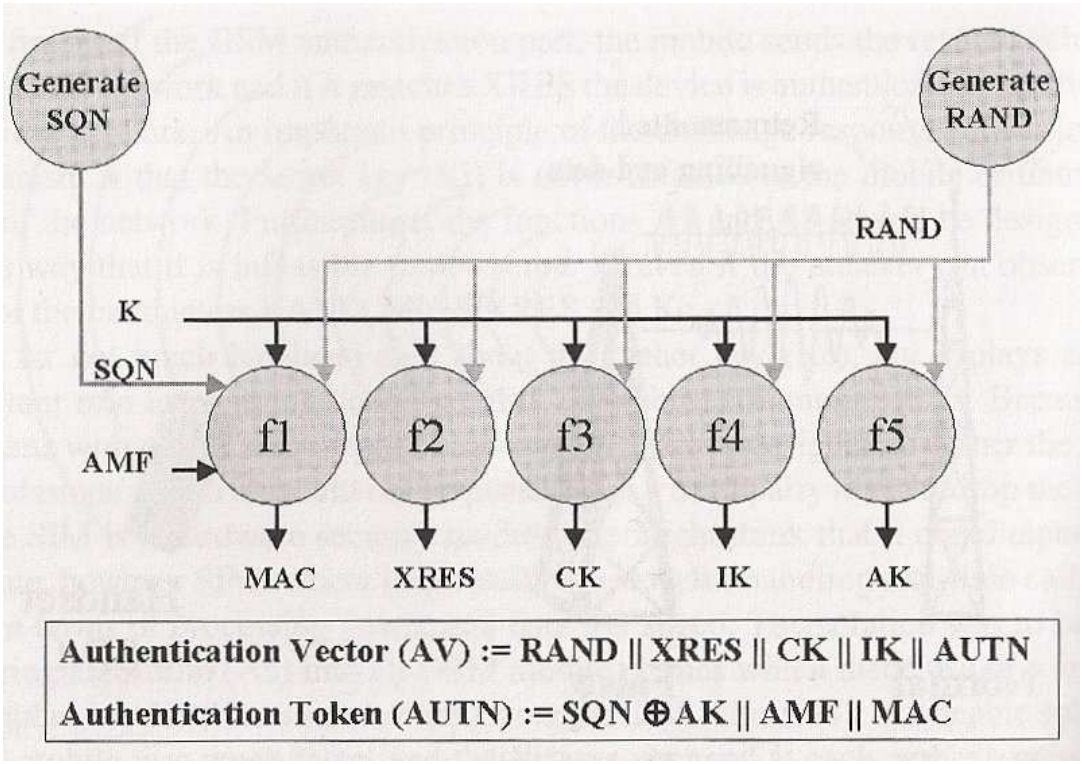
Kun mobiililaite käynnistetään SIM-kortin kanssa, se valitsee ensiksi SIM-kortilta MF-juuritiedoston. Kun taas mobiililaite käynnistetään ja UICC:lle on asennettu USIM, alkaa laite käyttää määrättyä USIM-sovellusta. Jos UICC:lle on asennettu myös SIM-sovellus, eikä käyttäjä tai mobiililaite sitä erikseen valitse, voi olla, että sitä ei ikinä käytetä. Mikäli EF_{DIR}-tiedostossa ei kuitenkaan ole tietoa USIM:sta, voi mobiililaite yrittää käyttää SIM:ä, jos se on asennettu. Myös usean USIM-sovelluksen ajaminen on mahdollista. Tällöin yhdellä älykortilla on mahdollista olla useampi puhelinnumero. Mikäli UICC:lla on useampi USIM-sovellus, täytyy käyttäjän valita aina, mitä sovellusta halutaan käyttää. Oletusarvona on, että viimeksi käytetty USIM-sovellus avataan. Tällöin käytetään ohjelmanvalintasovellusta AID:tä (Application Identifier), joka on varastoitu EF_{DIR}-tiedostoon. Myös useista eri käyttäjäprofiileja voidaan luoda USIM:lle mutta aina on oltava luotuna vähintään yksi. Kun USIM-sovellus on valittu, kysyy mobiililaite USIM:lta tiettyjä tietoja. Näitä ovat esimerkiksi yleinen hätänumero ja muut ETSI:n spesifikaatiossa TS 31.102 määrätyt tiedot. /7/

3.1.2 Autentikointi

Yksi suurimmista eroista SIM- ja USIM-korttien välillä on autentikointi. Yksinkertaisimmillaan autentikointi on salasanan tai PIN-koodin kysyminen ja sen oikeaksi toteaminen. SIM- ja USIM-tapauksissa näitä tunnuslukuja kutsutaan CHV-koodeiksi (Cardholder Verification). Seuraavassa käsitellään mobiililaitteen autentikoitumista verkkoon. Toisin sanoen verkko varmentaa, että mobiililaitteella on oikeus käyttää verkkoa ja päinvastoin. /2/

SIM- ja USIM-autentikoinnit on hyvin samanlainen prosessi ja tästä syystä näiden kahden välillä ei ole mitään suuria eroja. Voidaan sanoa, että USIM on tässäkin yhteydessä paranneltu versio SIM-kortista. Molemmissa, sekä SIM- että USIM-autentikoinneissa tarvitaan IMSI (International Mobile Subscriber Identity), joka on kortin tunnusnumero, salainen Ki-avain sekä varsinainen autentikointialgoritmi esimerkiksi A3 tai A8, joista yleisempi on A3. Nämä algoritmit voidaan yhdistää A38-algoritmiksi. /1, 2/

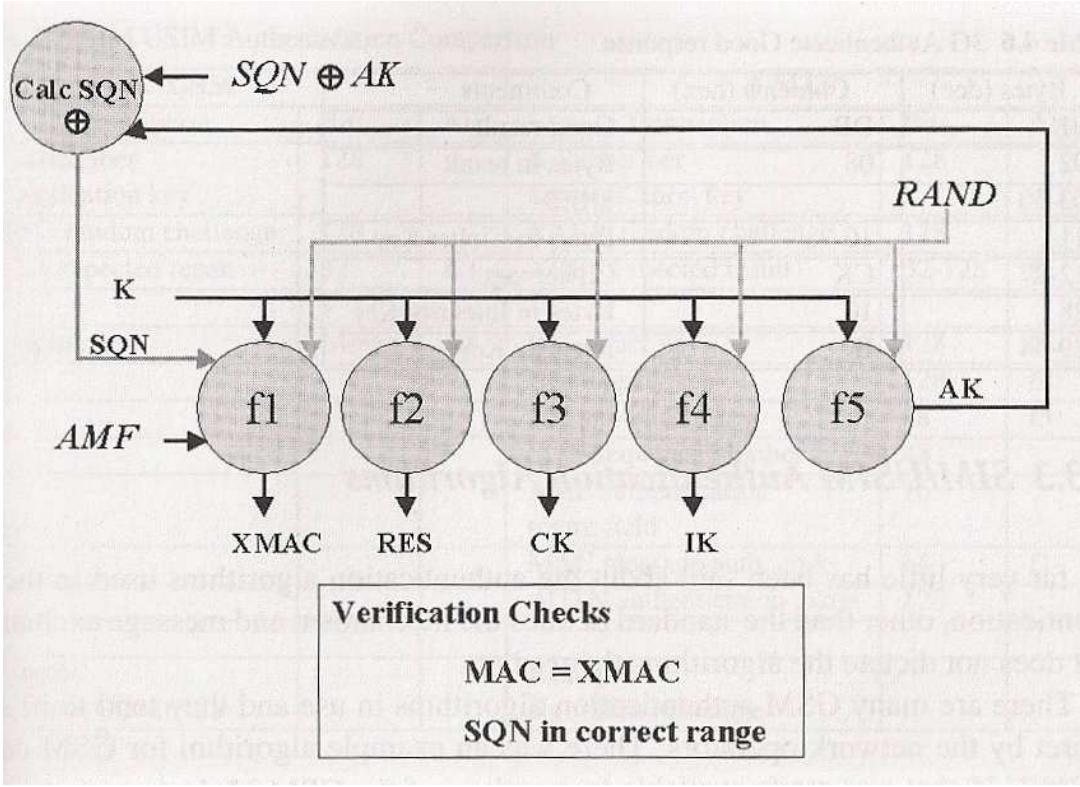
Yksi suurimmista eroista SIM- ja USIM-autentikoinnin välillä on se, että SIM-autentikoinnissa varmenneta ainoastaan SIM-kortti verkkoon, mutta verkkoa ei autentikoida millään tavalla. Näin ollen mobiililaite tai käyttäjä ei voi olla varma, onko kyseinen verkko varmasti luotettava. Mikäli mobiililaitteen ja verkon tukiaseman väliin asetetaan tukiasema, joka matkii verkkoa ja mobiililaitetta samalla välittäen viestit eteenpäin, mahdollistaa se kaiken liikkuvan datan seuraamisen. Tätä kutsutaan man-in-the-middle-hyökkäykseksi. Tässä tilanteessa väärän tukiaseman käyttäjä voi luoda, muuttaa tai estää datan välittymisen, joko mobiililaitteesta tukiasemaan tai päinvastoin. Pahimmillaan voidaan mobiililaitteelle kertoa että tässä ”verkossa” ei käytetä mitään salausta. Näin ollen laite lähettää kaiken datan täysin salaamattomana tukiasemalle, jossa se voidaan tulkita. Esimerkiksi tekstiviestin, joka sisältää vaikkapa verkkopankkitunnuksen, avaaminen voi johtaa merkittäviin väärinkäytöksiin. /1/



Kuva 1. UMTS-verkon autentikointi. /1/

Tämä puute on luonnollisesti korjattu USIM-autentikoinnissa siten, että varmennus tapahtuu kumpaankin suuntaan. Lisäksi kriittiset viestit, kuten käytetäänkö salausta vai ei, varmennetaan vielä eri metodilla. Tämä on toteutettu niin, että verkko luo salaisen K-avaimen avulla USIM:lle MAC:n (Message Authentication Code) eli avainnetun tiivistealgoritmin, jonka USIM sitten varmistaa. Mikäli MAC on oikein, USIM varmentaa verkon ja käyttää sitä. Tämän lisäksi verkossa käytetään myös jaksonumeroa (SQN). Tämän numeron on noudatettava tiettyä kaavaa, jotta USIM hyväksyy sen. /1, 2/

Kuvassa 1 on esitetty laskennat, joita verkko suorittaa USIM-korttia autentikoidessaan. Huomattakoon, että AV:ssä (Authentication Vector) eli autentikointivektorissa on UMTS-verkossa viisi osaa, kun GSM-verkossa siinä oli vain kolme. UMTS/USIM-autentikoinnissa käytetään myös kahta täysin uutta avainta verrattuna GSM/SIM-autentikointiin. Nämä avaimet ovat AUTN (Authentication Token), joka tukee molemminpuolista autentikointia sekä hallintaa ja IK (Integrity Key), jota käytetään suojaamaan verkon ja USIM-kortin välisiä viestejä. /1/



Kuva 2. USIM-kortin autentikointi /1/

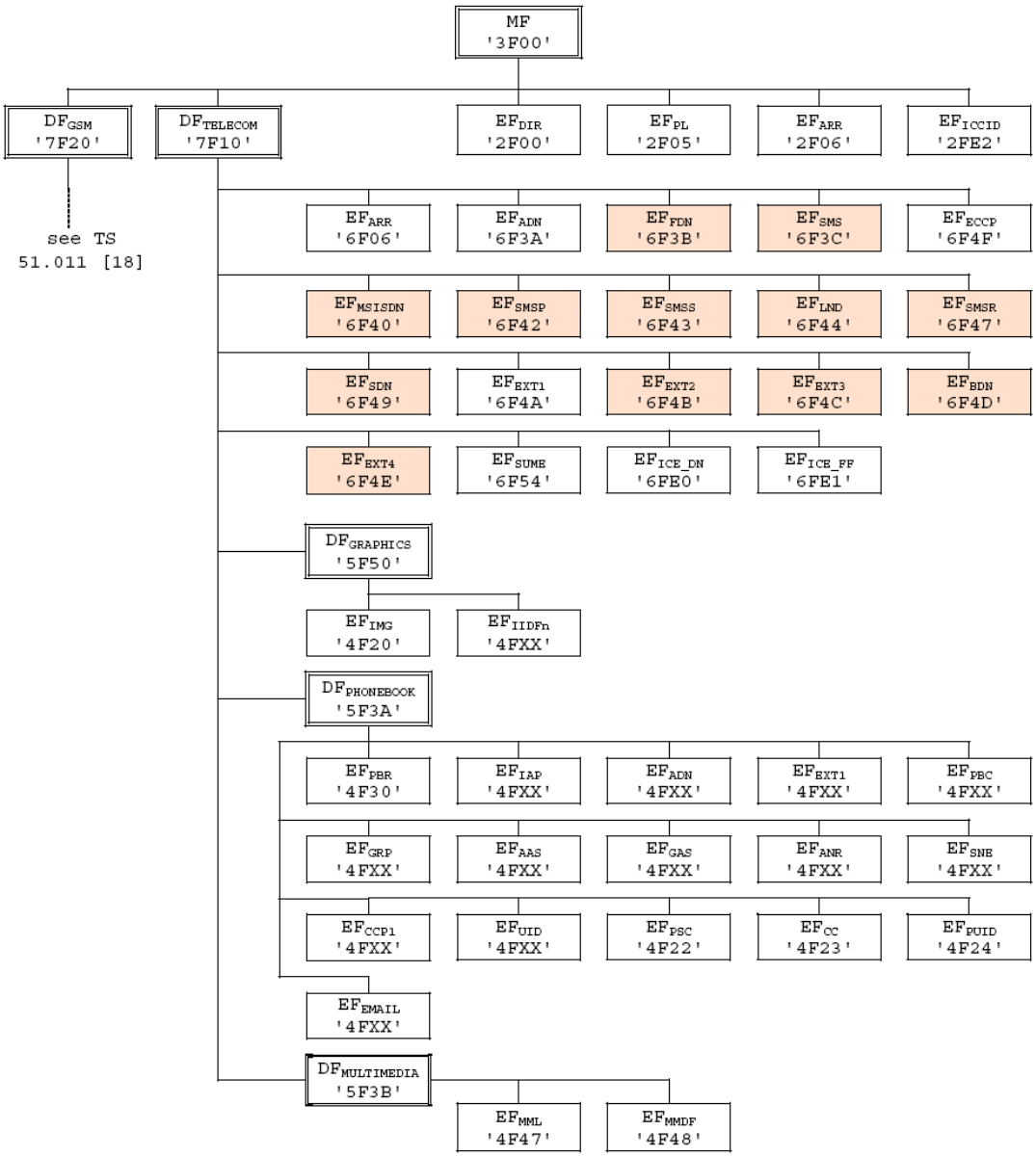
Niin GSM- kuin UMTS-autentikoinnissakin tärkeimpänä tekijänä voidaan pitää autentikointialgoritmejä. Näitä algoritmeja on olemassa monia, sillä monet matkapuhelinoperaattorit ovat kehittäneet omansa. Koska hyvä algoritmi pyritään aina pitämään tietoturvan vuoksi salaisena, on oikeastaan vaikea sanoa, kuinka monta algoritmia tänä päivänä on olemassa. Esimerkkinä algoritmin elämänkaaresta voidaan käyttää COMP128-algoritmia, jonka GSM MoU Association aikoinaan julkaisi. Monet operaattorit ottivat tämän hyväksi kokemansa algoritmin käyttöön. Pian ne kuitenkin huomasivat sen olevan niin sanotusti heikko ja verrattain helposti murrettavissa. Lisäksi COMP128:n turvallisuus riippui täysin algoritmin rakenteen salaisena pitämisestä. Kun algoritmi aikoinaan paljastui, sen tietoturva-arvo oli saman tien mennyttä.

ETSI julkaisi myöhemmin 3G:lle suunnitellun Milenage-algoritmin, joka ei ole riippuvainen varsinainen algoritmin rakenteen salassa pysymisestä. Milenage perustuu julkisesti vahvaksi havaittuun AES-algoritmiin. Milenage-algoritmi on tehty myös GSM:lle ja kulkee nimellä G-Milenage.

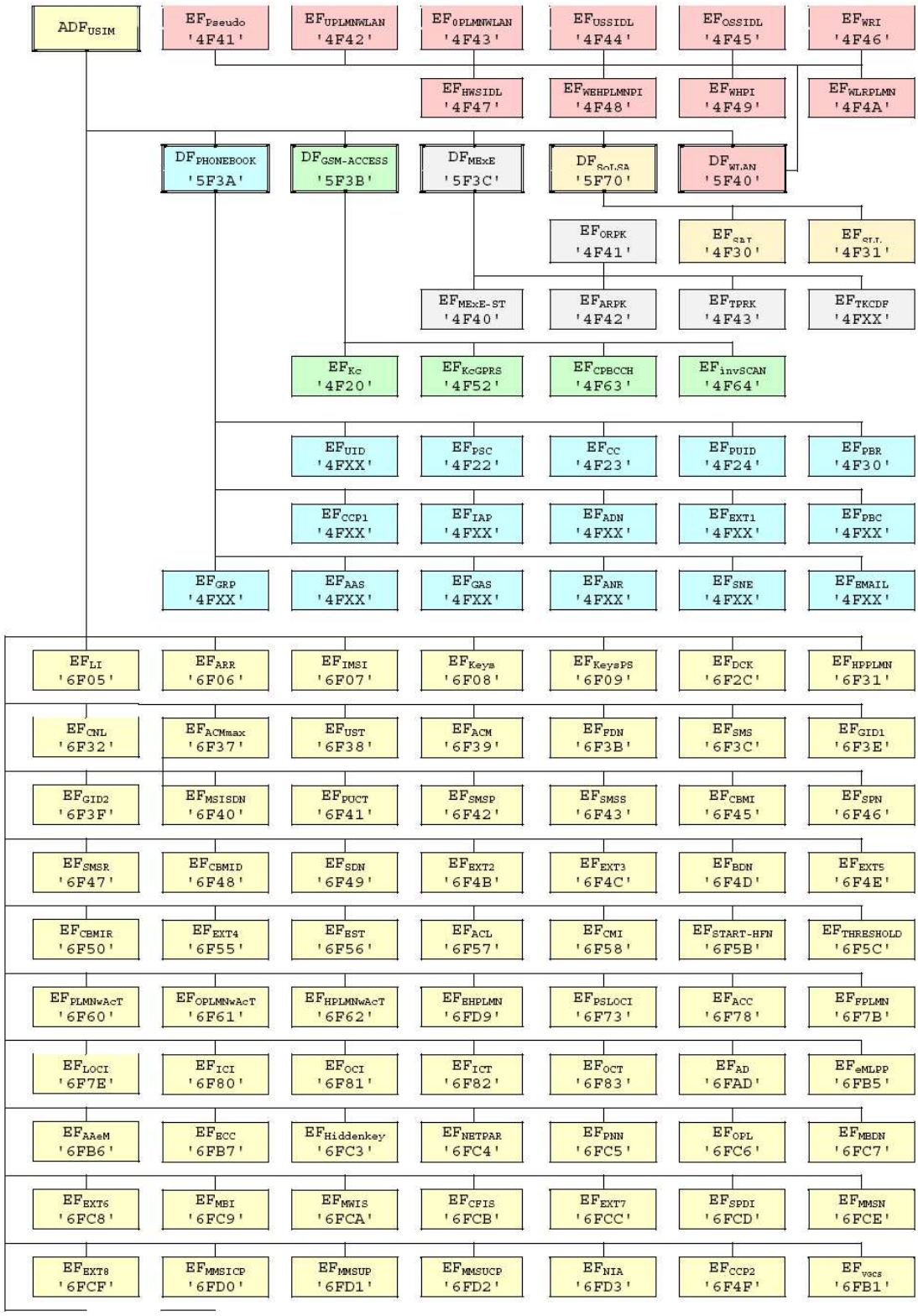
3.1.3 Tiedostorakenne

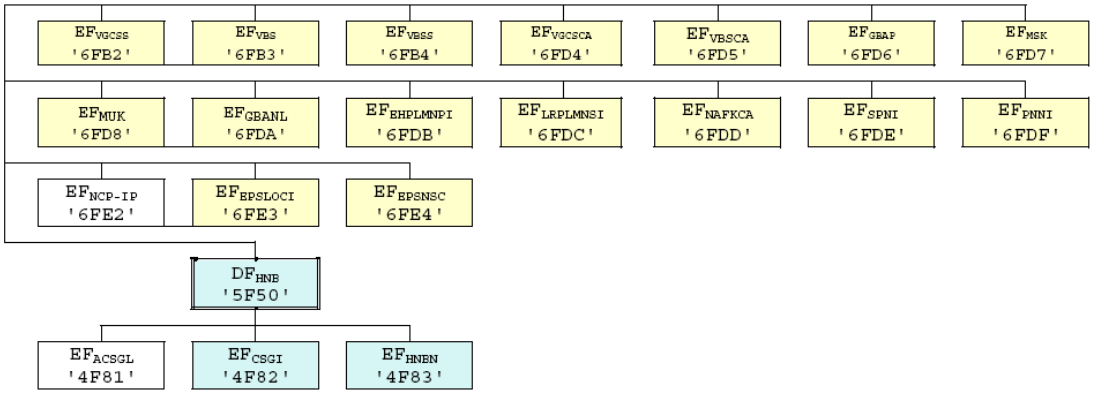
USIM-kortilla tiedostorakenne täytyy jakaa varsinaisen USIM-ohjelman ja UICC-alustan välille. Molemmilla on omat tiedostonsa ja tiedostorakenteensa. Näiden kahden eroa voidaan kuvata helposti EF_{IMSI}-tiedostolla. Tämä tiedosto löytyy USIM-tiedostorakenteen alta. Vastaavasti $DF_{GSM\ ACCESS}$-alikansioista löytyvät autentikointiin tarvittavat avaimet esimerkiksi EF_{Kc}-tiedosto.

Osa tiedostoista näkyy molemmissa tiedostorakenteista, tästä esimerkkinä EF_{MSISDN}-tiedosto.



Kuva 3. UICC:n tiedostorakenne /7/


ADF USIM
EF Pseudo '4F41'
EF UPLMNWLAN '4F42'
EF OPLMNWLAN '4F43'
EF USSIDL '4F44'
EF OSSIDL '4F45'
EF WRI '4F46'
EF HWSIDL '4F47'
EF WEHPLMNPI '4F48'
EF WHPI '4F49'
EF WLRPLMN '4F4A'
DF PHONEBOOK '5F3A'
DF GSM-ACCESS '5F3B'
DF MExE '5F3C'
DF SoLSA '5F70'
DF WLAN '5F40'
EF ORPK '4F41'
EF SAT '4F30'
EF SAT '4F31'
EF MExE-ST '4F40'
EF ARPK '4F42'
EF TPRK '4F43'
EF TKCDF '4FXX'
EF Kc '4F20'
EF KcGPRS '4F52'
EF CPBCCH '4F63'
EF invSCAN '4F64'
EF UID '4FXX'
EF PSC '4F22'
EF CC '4F23'
EF PUID '4F24'
EF PBR '4F30'
EF CCP1 '4FXX'
EF IAP '4FXX'
EF ADN '4FXX'
EF EXT1 '4FXX'
EF PBC '4FXX'
EF GRP '4FXX'
EF AAS '4FXX'
EF GAS '4FXX'
EF ANR '4FXX'
EF SNE '4FXX'
EF EMAIL '4FXX'
EF LI '6F05'
EF ARR '6F06'
EF IMSI '6F07'
EF Keys '6F08'
EF KeysPS '6F09'
EF DCK '6F2C'
EF HPPLMN '6F31'
EF CNL '6F32'
EF ACMmax '6F37'
EF UST '6F38'
EF ACM '6F39'
EF FDN '6F3B'
EF SMS '6F3C'
EF GID1 '6F3E'
EF GID2 '6F3F'
EF MSISDN '6F40'
EF PUCT '6F41'
EF SMSP '6F42'
EF SMSS '6F43'
EF CBMI '6F45'
EF SPN '6F46'
EF SMSR '6F47'
EF CBMID '6F48'
EF SDN '6F49'
EF EXT2 '6F4B'
EF EXT3 '6F4C'
EF BDN '6F4D'
EF EXT5 '6F4E'
EF CBMIR '6F50'
EF EXT4 '6F55'
EF EST '6F56'
EF ACL '6F57'
EF CMI '6F58'
EF START-HFN '6F5B'
EF THRESHOLD '6F5C'
EF PLMNwAcT '6F60'
EF OPLMNwAcT '6F61'
EF HPLMNwAcT '6F62'
EF EHPLMN '6FD9'
EF PSLOCI '6F73'
EF ACC '6F78'
EF FPLMN '6F7B'
EF LOCI '6F7E'
EF ICI '6F80'
EF OCI '6F81'
EF ICT '6F82'
EF OCT '6F83'
EF AD '6FAD'
EF eMLPP '6FB5'
EF AAeM '6FB6'
EF ECC '6FB7'
EF Hiddenkey '6FC3'
EF NETPAR '6FC4'
EF PNN '6FC5'
EF OPL '6FC6'
EF MBDN '6FC7'
EF EXT6 '6FC8'
EF MBI '6FC9'
EF MWIS '6FCA'
EF CFIS '6FCB'
EF EXT7 '6FCC'
EF SPDI '6FCD'
EF MMSN '6FCE'
EF EXT8 '6FCF'
EF MMSICP '6FD0'
EF MMSUP '6FD1'
EF MMSUCP '6FD2'
EF NIA '6FD3'
EF CCP2 '6F4F'
EF VGCS '6FB1'



Kuva 4. USIM-tiedostorakenne /7/

USIM:lta löytyvät tiedostot ovat monilta osin samat kuin SIM-kortillakin. Kuitenkin yksi tärkeä lisäys EF_{ARR}-tiedosto (Access Rule Reference). Tähän tiedostoon on määritelty USIM ADF-kansion (Application DF) tai Telecom puolella $DF_{TELECOM}$-alikansion pääsyrajoitukset. Mikäli EF_{ARR}-tiedostoa ei voida lukea, ja siihen on tehty määrityksiä, kaikki pääsyt kyseisiin alikansioihin estetään. /2, 7/

EF_{UST}-tiedosto (USIM Service Table) on pakollinen tiedosto, josta käy ilmi käytettävissä olevat toiminnot. Mikäli toiminto ei ole USIM:lla käytettävissä, ei mobiililaite sitä myöskään valitse. Tällaisia toimintoja ovat esimerkiksi paikallinen puhelinluettelo, palveluntarjoajan tiedot ja multimediaviestien tallennus. Mikäli palvelu on merkitty mahdolliseksi, USIM-kortti tukee tällöin palvelua ja se voidaan ottaa käyttöön. /7/

EF_{ECC}-tiedostossa (Emergency Call Codes) on listattu hätänumerot, joihin käyttäjä voi soittaa ilman PIN-koodia. Tämä käy ilmi tiedoston READ- eli lukuoikeudesta, joka on aina ALW-tilassa (Always). Tässä tilassa tiedosto on aina luettavissa. Tämä tiedosto on USIM-spesifikaation mukaan pakollinen, mitä se ei SIM-korteilla ollut. /7/

$EF_{START\text{-}HFN}$-tiedosto (Initialisation values for Hyperframe number) sisältää $START_{CS}$- ja $START_{PS}$-arvot, joita käytetään Hyperframe-arvon luonnissa. $EF_{THRESHOLD}$-tiedosto puolestaan määrittelee $START_{CS}$- ja $START_{PS}$-arvojen voimassaoloajat. /7/

EF_{NETPAR}-tiedosto (Network Parameters) sisältää tietoja, liittyen matkapuhelinverkkojen solujen taajuuksiin. Tähän tiedostoon voidaan tallentaa tietty taajuus, jota USIM:n halutaan käyttävän. Tämän johdosta osa verkon soluista voidaan rajata haun ulkopuolelle, näin ollen nopeuttaen ja rajaten solun löytymistä. Taajuudet voivat vaihdella 0-13,1 GHz välillä, 200 kHz portailla. /7/

Kaikki ylläluettelut tiedostot ovat ETSI:n spesifikaation TS 31.102 mukaan pakollisia tiedostoja, joiden tulee sijaita USIM-kortilla. Näiden tiedostojen lisäksi kortilla voi olla myös monia valinnaisia tiedostoja. Niitä lisätään kortille aina sen mukaan, mitä kortilla halutaan tehdä ja mitä toimintoja sen halutaan tukevan. Tällainen tiedosto voi olla esimerkiksi EF_{MMSICP} (MMS Issuer Connectivity Parameters), jossa on määritykset joita mobiililaite käyttää ottaessaan yhteyttä MMS:ään (Multimedia Messaging Service) eli multimediaviestien palvelimeen. /7/

3.1.4 Toiminnot

USIM:n alakansioina voi esiintyä monia eri sovelluksia ja toimintoja. $DF_{GSM\text{-}ACCESS}$-kansion sisältönä on muun muassa Kc-avain. DF_{WLAN}-kansiossa on WLAN-käyttöön (Wireless Local Area Network) eli langattomaan lähiverkkoon tarkoitettuja tiedostoja. Näistä esimerkkinä on väliaikaisen tunnistetiedon WLAN-yhteyttä varten tarkoitettu EF_{PSEUDO}-tiedosto (Pseudonym). /7/

Muitakin kansioita voi sijaita USIM:lla. Näistä käyttäjälle kaikista näkyvin on kuitenkin puhelinluettelo. /1, 7/

Puhelinluettelo

ETSI:n spesifikaatiossa TS 21.111 määritellään USIM:n puhelinluettelolle tiettyjä vaatimuksia, joita sen on pystyttävä toteuttamaan. Esimerkkeinä näistä ovat kahden nimen käyttö, yhdelle nimelle pitää pystyä määrittämään monta numeroa, sähköpostiosoite on pystyttävä liittämään numeroon ja kortille on pystyttävä tallentamaan vähintään 500 numeroa. /7/

UICC:lla saattaa olla oma puhelinluettelo, joka sijaitsee sen $DF_{PHONEBOOK}$-alikansiossa. Myös sovelluskohtaisia puhelinluetteloita voi olla tallennettu UICC:lle. USIM:n tapauksessa ne sijaitsevat aina USIM:n omassa tiedostorakenteessa AD-F_{USIM}-kansion $DF_{PHONEBOOK}$-alikansiossa. Nämä puhelinluettelot toimivat aina erillään, täysin tietämättöminä toisistaan. Siksi onkin suotavaa, että mobiililaite etsii ensin mahdollisen UICC:lla sijaitsevan puhelinluettelon, koska USIM-sovellus ei sitä automaattisesti tee. Mikäli UICC:lla on useampi USIM-sovellus, voi niistä jokaisella olla oma puhelinluettelo. Nämä sijaitsevat kyseisen USIM-sovelluksen omassa $DF_{PHONEBOOK}$-kansiossa. /7/

Jos UICC:lla on myös GSM-sovellus ja jokin puhelinluettelo on linkitetty tähän sovellukseen, voidaan kyseinen puhelinluettelo valita GSM-sovelluksen kautta. Toisin sanoen $DF_{PHONEBOOK}$-kansion tiedot linkitetään kyseiseen $DF_{TELECOM}$-kansioon. /7/

$DF_{TELECOM}$-kansiossa on aina oltava vähintään EF_{ADN}-tiedosto (Abbreviated Dialing Numbers), joka sisältää itse puhelinnumeron, sekä EF_{PBR}-tiedosto (Phone Book Reference file), joka sisältää puhelinluettelon rakenteelliset tiedot. Mikäli puhelinluettelossa halutaan käyttää muitakin tietoja kuin pelkkää puhelinnumeroa, täytyy kansiossa olla myös niihin liittyvät tiedostot. Esimerkiksi, jos puhelinnumeroon halutaan liittää sähköpostiosoite, on sen tiedot tallennettu EF_{EMAIL}-tiedostoon (e-mail address). /7/

3.2 Yhteensopivuus

ETSI:n määrittelemän spesifikaation mukaan UMTS:n järjestelmien tulee mahdollistaa roaming-toiminto GSM-verkoissa. Tämä tarkoittaa, että USIM-kortin UICC:n tulee toimia kaksoistilassa, jossa toisessa toimii USIM/3G-järjestelmä ja toisessa GSM/2G-järjestelmä. Tämä on toteutettu USIM-kortilla niin, että UICC:lla toimii samanaikaisesti sekä USIM- että GSM-sovellus. Näin ollen 3G-matkapuhelinverkkoa tukevien korttien ja puhelimien tulee tukea myös 2G-matkapuhelinverkkoja. Sama toimii myös toiseen suuntaan. ETSI:n spesifikaatioiden mukaan 3G-verkon rakenteen on tuettava SIM-korttia. /6, 1/

4 ÄLYKORTIN LUKULAITE JA –OHJELMA

Tässä opinnäytetyössä käytetty lukulaite on Gemalto PC Twin Reader (USB). Ohjelma lukulaitetta varten on Gemalto Telecom Card Administrator v1.6, josta käytetään lyhennettyä nimeä Card Admin. /5/

4.1 Asennus

Ohjelman tämä versio soveltuu vain Windows 2000- ja Windows XP-käyttöjärjestelmille, esimerkiksi Windows Vistaan versiota 1.6 ei tällä hetkellä saa asennettua. Ennen varsinaisen ohjelman asennusta tulee asentaa asennuslevyltä löytyvät ajurit kortinlukijalle sekä Java Development Kit-ohjelma. Molemmat löytyvät asennuslevyltä omista kansioistaan. Niistä löytyy asennustiedosto, jolla asennus käynnistyy. Mikäli tietokone tunnistaa kortinlukijan, ei ajureita välttämättä tarvitse asentaa. On kuitenkin suositeltavaa käyttää valmistajan tarjoamia ajureita, mikäli mahdollista. Tietokoneelle voi myös olla jo asennettu Java Development Kit. Jos tästä ei ole varmuutta, asennetaan ohjelma asennuslevyltä.

Näiden asennusten jälkeen voidaan asentaa itse Card Admin-ohjelma. Asennusohjelma käynnistetään asennuslevyn tiedostosta setup.exe tai se käynnistyy automaattisesti, kun asennuslevy laitetaan asemaan. Asennusohjelma saattaa muistuttaa, että tietyt ajurit eivät ole ajan tasalla, mutta tästä ei tarvitse huolestua. On suositeltavaa asentaa Card Admin-ohjelma asennusohjelman ehdottamaan kansioon. Kun asennusohjelma kysyy mitä laitteita halutaan käyttää, painetaan ensin Select All-nappia ja sitten jatketaan Next-napilla. Tämän jälkeen asennusohjelma varmistaa haluatko varmasti asentaa sen. Tähän painetaan Install-nappia. Ohjelma alkaa asentumaan tietokoneelle. Kun asennus on valmis, täytyy tietokone käynnistää uudestaan. Tämän jälkeen Card Admin-ohjelma on käyttövalmis.

4.1.1 Lisenssi

Kun ohjelma käynnistetään ensimmäistä kertaa, se kysyy käyttäjän lisenssitiedostoa. Mikäli lisenssitiedosto on tilattu käytössä olevalle koneelle, se voidaan syöttää ohjelmaan painamalla Import License-nappia. Tämän jälkeen haetaan lisenssitiedosto ja valitaan se. Ohjelma on tämän jälkeen rekisteröity ja se näyttää milloin lisenssi umpeutuu. Mikäli lisenssitiedostoa ei ole ja se halutaan luoda, painetaan tällöin Export License-nappia. Tällöin ohjelma luo haluttuun kansioon xml-tiedoston, joka voidaan lähettää valmistajalle. On tärkeää huomata, että lisenssitiedosto on tietokonekohtainen ja toimii ainoastaan sillä tietokoneella, jolla valmistajalle lähetetty xml-tiedosto on luotu. Mikäli lisenssitiedostoa ei ole, voidaan aloittaa 20 päivän kokeilujakso valitsemalla Close-nappi.

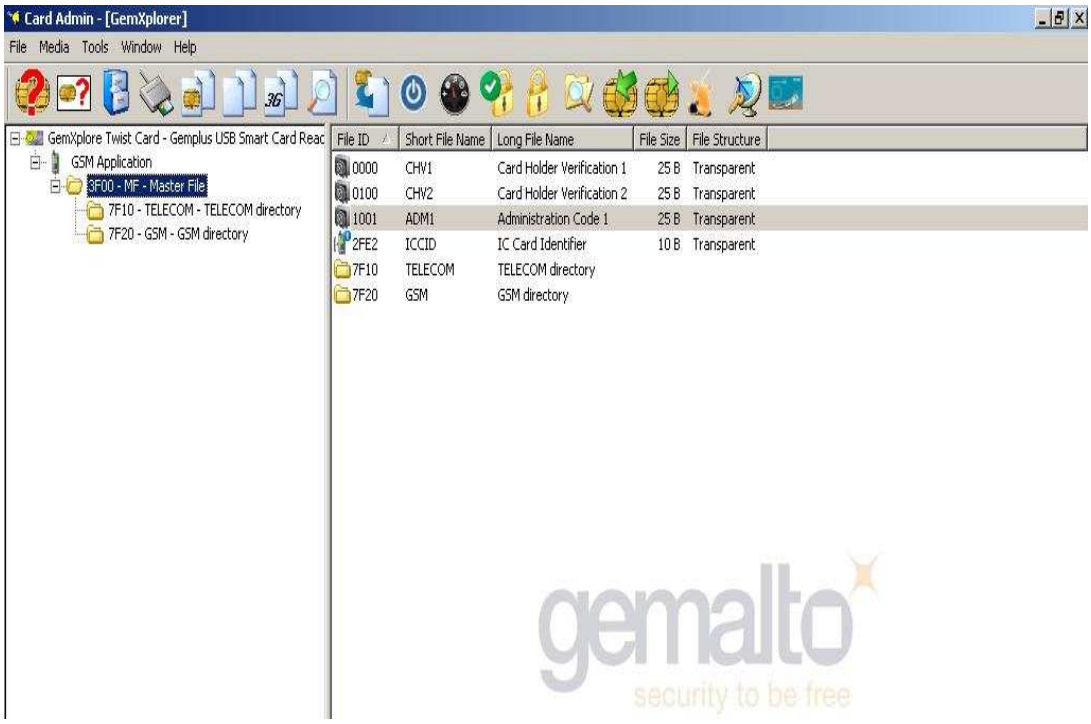
4.2 Käyttö

Card Admin-ohjelma käynnistetään pikakuvakkeesta, jonka asennusohjelma luo Windowsin työpöydälle. Ohjelman avauduttua voi kortinlukijaan syöttää luettavan älykortin. Ohjelma yrittää tunnistaa kortin. Jos ohjelma onnistuu siinä, pääsee käyttäjä käsittelemään kortin tietoja suoraan. Mikäli ohjelma ei tunnista korttia, joutuu käyttäjä valitsemaan kortin listalta tai luomaan sen itse. Tässä työssä käytetty kortti oli Satakunnan ammattikorkeakoulun 2G+-kortti, jota ohjelma ei tunnistanut. GemXplore Twist Card-kortti vastasi kuitenkin kortin ominaisuuksia, joten näitä asetuksia käytettiin.

4.2.1 SIM- ja USIM-tilan käyttö

SIM- ja USIM-tiloissa voi kortin tiedostoja lukea ja muokata, mikäli käyttäjällä on siihen oikeudet. Nämä toiminnot voivat vaatia joko CHV- tai ADM-koodeja. Kaikki kortin käyttämät koodit voidaan syöttää valmiiksi valitsemalla ylävalikosta Verify Code-painike. Tämän jälkeen voidaan syöttää haluttu koodi ja painaa Verify-painiketta. Mikäli koodi on oikein, ikkunan alareunaan tulee lukemaan Success.

Koodin vieressä näkyy Block-laskuri, josta näkee kuinka monta kertaa koodin saa syöttää väärin. Mikäli laskuri on nollassa, koodi on lukittu ja se täytyy avata. Tämä tehdään valitsemalla Unblock-välilehti ja syöttämällä tarvittava koodi. Esimerkiksi CHV1-koodin (PIN1) avaa PUK2-koodi. Disable-välilehdellä koodin kysymisen voi poistaa täysin ja Re-enable-välilehdellä laittaa kyselyn takaisin päälle. Tässä on tärkeää huomioida, että kortti voi lukittua myös tässä ohjelmassa, samoin kuin puhelimessakin. Tästä syystä CHV- ja ADM-koodeja ei kannata syöttää turhaan, mikäli niitä ei ole tiedossa.



Kuva 5. Card Admin SIM-tila

Kuvassa 5 näkyy Card Admin-ohjelman SIM- ja USIM-tilan perustila. Vasemmassa sarakkeessa näkyy kortin kansiorakenne. Ylimpänä näkyy itse kortti, sitten kortin alikansiot ja sovellukset. Kun kansio on valittu, näkyy oikeassa sarakkeessa kansion sisältämät alikansiot ja tiedostot.

File ID	Short File Name	Long File Name	File Size	File Structure
6F3A	ADN	Abbreviated Dialing Numbers	5100 B	Linear-fixed
6F3B	FDN	Fixed Dialing Numbers	360 B	Linear-fixed
6F3C	SMS	Short Message Service	3520 B	Linear-fixed
6F3D	CCP	Capability Configuration Parameters	56 B	Linear-fixed
6F40	MSISDN	Mobile Subscriber Identity Dialing Number	64 B	Linear-fixed
6F42	SMSP	Short Message Service Parameters	80 B	Linear-fixed
6F43	SMSS	Short Message Service Status	2 B	Transparent
6F44	LND	Last Number Dialed	340 B	Cyclic
6F49	SDN	Service Dialing Numbers	120 B	Linear-fixed
6F4A	EXT1	Extension 1	65 B	Linear-fixed
6F4B	EXT2	Extension 2	26 B	Linear-fixed
6F4C	EXT3	Extension 3	26 B	Linear-fixed

Kuva 6. Kansion 7F10 eli Telecom-kansion tiedostot

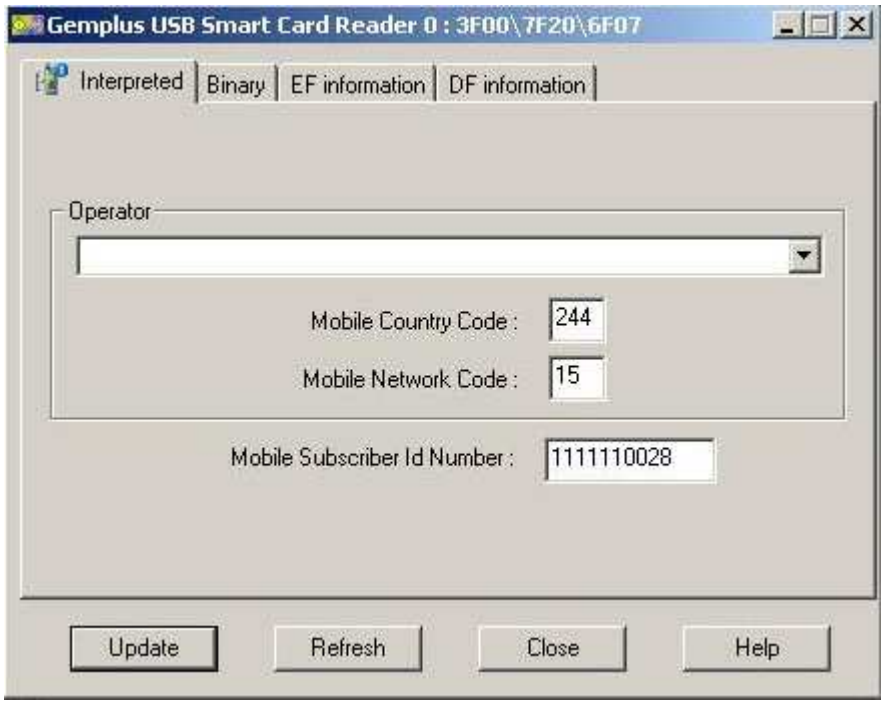
Kuvassa 6 näkyvät 7F10-kansion eli Telecom-kansion tiedostot. Tästä kansiosta löytyvät esimerkiksi tiedosto, johon tekstiviestit tallennetaan. Sarakkeessa näkyvät vasemmalta oikealle lukien sarakkeet File ID eli nimi, jolla tiedosto on tallennettu kortille. Card Admin tulkitsee nämä nimet määriteltyjen standardien mukaisesti niin, että käyttäjä voi lukea tiedoston lyhenteen ja koko nimen seuraavista sarakkeista. Esimerkiksi 6F44-tiedoston lyhenne on LND eli Last Number Dialed. Tästä tiedostosta näkyy viimeksi soitettu numero.

File ID	Short File Name	Long File Name	File Size	File Structure
0001	Key-op	Applicative Key	73 B	Transparent
6F05	LP	Language Preference	5 B	Transparent
6F07	IMSI	International Mobile Subscriber Identifier	9 B	Transparent
6F20	Kc	Ciphering Key Kc	9 B	Transparent
6F30	PLMNsel	Public Land Mobile Network Selector	60 B	Transparent
6F31	HPPLMN	Home Public Land Mobile Network Search period	1 B	Transparent
6F37	ACMmax	Accumulated Call Meter max. Value	3 B	Transparent
6F38	SST	SIM Service Table	13 B	Transparent
6F39	ACM	Accumulated Call Meter	30 B	Cyclic
6F41	PUCT	Price per Unit and Currency Table	5 B	Transparent
6F45	CBMI	Cell Broadcast Msg. Identifier Selection	10 B	Transparent
6F46	SPN	Service Provider Name	17 B	Transparent
6F52	KcGPRS	Ciphering Key KcGPRS	9 B	Transparent
6F53	LOCIGPRS	GPRS Location Information	14 B	Transparent
6F74	BCCH	Broadcast Command Channels	16 B	Transparent
6F78	ACC	Access Control Class	2 B	Transparent
6F7B	FPLMN	Forbidden Public Land Mobile Network	12 B	Transparent
6F7E	LOCI	Location Information	11 B	Transparent
6FAD	AD	Administrative Data	3 B	Transparent
6FAE	Phase	Phase Identification	1 B	Transparent

Kuva 7. Kansion 7F20 eli GSM-kansion tiedostot

Kuvassa 7 näkyvät 7F20-kansion eli GSM-kansion tiedostot. Tästä kansiosta löytyvät varsinaiseen puheluun liittyvät tiedostot, esimerkiksi 06F7 (IMSI), 6F20 (Kc-avain).

Kun tiedostoja halutaan lukea, tapahtuu se tuplaklikkaamalla niitä hiiren vasemmalla napilla. Tiedosto aukeaa ja siihen voi tehdä muutoksia, mikäli oikeudet ovat kunnossa. Kun tehdyt muutokset halutaan tallentaa kortille, painetaan Update-näppäintä. On tärkeää huomata, että kun muutos on tehty, se tallentuu suoraan kortille. Mikäli muutos tämän jälkeen halutaan peruuttaa, on vanha arvo syötettävä uudelleen tiedostoon.



Kuva 8. Tiedoston 6F07 (IMSI) ominaisuuksien muutosikkuna

Kuvassa 8 näkyy esimerkkinä IMSI-tiedoston ominaisuuksien muutosikkuna. Tästä ikkunasta voidaan määrittää kortin matkapuhelinoperaattori, maakoodi, matkapuhelinverkon koodi ja itse IMSI-numero. Alareunassa näkyy Update-painike, jolla muutokset asetetaan kortille. Close-painikkeella voi puolestaan poistua tekemättä muutoksia. Yläreunan välilehdissä on samat tiedot eri muodoissa. Binary-välilehdellä tiedot esitetään binäärimuotoisena. EF-information eli tiedosto-välilehdellä esitetään tietoa itse tiedoston käyttöoikeuksista ja muista ominaisuuksista. DF- eli alihakemisto-välilehdellä esitetään vastaavat tiedot kuin EF-välilehdellä, mutta alihakemiston näkökulmasta.

Kuva 9. Card Admin työkalurivi

Card Admin ohjelman työkaluriviltä löytyvät ohjelman tärkeimmät komennot. Näillä komennoilla saadaan luotua kortista raportti, jota voidaan sitten verrata ohjelman avulla toisen kortin vastaavaan raporttiin. Verify All Pins-komennolla voidaan syöttää kaikki CHV- ja ADM-koodit kerralla. Network Authentication Aplication–komennolla voidaan testata kortin autentikointia.

4.2.2 Image-kortin luonti

Card Adminissa on mahdollista luoda ns. Image-kortti. Tämä kortti on tietokoneelle tallennettu tiedosto, joka on oikeastaan vain kuva (eng. image) oikeasta fyysisestä kortista. Image-kortilla on mahdollista harjoitella tiedostojen käsittelyä ja vaikkapa IMSI-numeron muuttamista, ilman fyysisen kortin toimimattomaksi tekemisen pelkoa.

Image-kortti luodaan valitsemalla Media valikosta Media Management. Tämän jälkeen File-välilehdellä painetaan Add-nappia ja valitaan vaihtoehto New. Seuraavaksi avautuu ikkuna, jossa ohjelma kysyy kortin tallennuspaikkaa ja -nimeä.

Image-kortille voi lisätä tiedostoja kahdella tavalla. Jos käyttäjä tietää minkä tiedoston hän haluaa lisätä, sen voi tehdä napsauttamalla hiiren oikealla painikkeella oikeanpuoleiseen hakemistoalueeseen. Tästä valitaan Create-vaihtoehto, jonka jälkeen valitaan tiedosto, joka halutaan lisätä. Toinen keino on kopioida tiedosto olemassa olevalta fyysiseltä kortilta tai toiselta image-kortilta. Tämä tapahtuu vetämällä tiedosto kortilta toiselle, käyttäen hiiren vasenta nappia.

Tiedostojen ominaisuuksia voi muokata valitsemalla ensin tiedosto oikeanpuoleisesta hakemistoalueesta ja sitten oikealla hiiren napilla valitsemalla Edit Properties. Tästä

aukeaa ikkuna, jossa käyttäjä voi muuttaa esimerkiksi tiedoston kokoa ja luku- ja kirjoitusoikeuksia. Fyysisille korteille tätä ei voi tehdä, koska arvot säädetään kortin valmistuksen yhteydessä.

Huomioitavaa on, että kaikki tehdyt muutokset tallentuvat automaattisesti image-kortille, ilman erillistä tallennusta. Käyttäjän täytyy siis olla varma tekemistään muutoksista. Sama pätee myös fyysisiin kortteihin.

Image-kortin avulla voi myös fyysisen kortin tiedot kopioida toiselle fyysiselle kortille. Tämä on tehtävä nimenomaan image-kortin avulla, koska Card Admin-ohjelma ei salli kopioida kahta fyysistä korttia suoraan keskenään. Kun tiedostot on kopioitu fyysiseltä kortilta image-kortille, voidaan niiden arvoja muokata ja esimerkiksi IMSI-arvoa muuttaa. Myös tiedoston oikeuksia voidaan muuttaa tässä yhteydessä, esimerkiksi luku- ja kirjoitusoikeudet voidaan poistaa. Näitä muutoksia tehtäessä ja tiedostoja kopioidessa on huomioitava korttien samankaltaisuus. Eri korttien tiedostot voivat poiketa kooltaan toisistaan ja näin ollen eivät ole välttämättä suoraan yhteensopivia toisten korttien kanssa. Tiedostoja voi kopioida myös useita kerrallaan, mikäli ne sijaitsevat samassa kansiossa.

Mikäli tiedostolle ei ole lukuoikeuksia (Read), sitä ei myöskään voi kopioida toiselle kortille. Toisaalta myös kohteena olevalle kortille on oltava lupa joko päivittää (Update) tai luoda (Create) uusia tiedostoja. Molemmat näistä ehdoista on otettava huomioon tiedostoja kopioidessa. Kopioinnin alkaessa Card Admin-ohjelma avaa kopiointi-ikkunan. Mikäli kopiointi onnistuu, tulee näkyviin vihreä merkki. Jos näkyviin tulee keltainen merkki, on tiedosto suojattu esimerkiksi CHV1-koodilla (PIN1). Tiedosto kopioituu, mutta sen sisältö ei. Tämä korjataan avaamalla tiedosto ja syöttämällä CHV1-koodi. Punainen merkki tarkoittaa, että kopiointi on epäonnistunut.

4.2.3 Autentikointi

Card Admin-ohjelmalla voidaan testata myös SIM-kortin autentikoitumista verkkoon. Autentikointi suoritetaan käynnistämällä Network Authentication Application työkalurivin oikeasta laidasta.

Autentikoinnin voi suorittaa joko avustetulla kohta-kohdalta-toiminnolla, jossa käyttäjältä kysytään esimerkiksi IMSI-arvo, tai nopeammalla yhden kohdan toteutuksella.

Avustetussa versiossa voidaan käyttää ainoastaan XOR-algoritmia. Nopeammassa ja yksiselitteisemmässä versiossa voi käyttäjä itse valita haluamansa algoritmin, esimerkiksi Milenage-algoritmin.

5 YHTEENVETO

Opinnäytetyössä olen tutkinut älykortin lukulaitetta ja sen Card Admin-sovellusta. Tähän liittyen perehdyin USIM-kortin ominaisuuksiin, verrattuna lähinnä SIM-korttiin. Työssä havaitsin, että USIM-kortti on huomattavasti kehittyneempi versio SIM-kortista.

Mielestäni on harhaanjohtavaa puhua USIM-kortista samoin kuin SIM-kortista, sillä niillä on todella suuri rakenteellinen ero. Kuten teoriaosuudessa käy ilmi, on USI sovellus, jota ajetaan älykortilla. Tämän sovelluksen alustana toimii UICC. Yleisesti puhekielessä käytetään termiä USIM-kortti, mikä on sinänsä hyvä, koska se on selkeä ja melko vakiintunut ilmaus. On kuitenkin hyvä muistaa, että USIM ei ole fyysinen kortti, vaan sovellus. Ehkä olisi oikeampi puhua UICC-kortista.

Käyttämäni lukulaite ja sen sovellus ovat pienen tutustumisen jälkeen erittäin hyvät työkalut älykortteihin tutustumisessa. Lukulaite toimii varmasti ja helposti. Itse sovelluksessa on havaittavissa joskus niin sanottua ”kaatumista”, eli ohjelma lopettaa toimintansa ja sammuu. Tätä tapahtuu kuitenkin melko harvoin. Koska tiedot on aina ladattavissa takaisin kortilta, joko fyysiseltä tai imagelta, ei kaatuilu haittaa varsinaista työskentelyä paljoakaan.

Voin siis todeta, että Gemalton Card Admin ohjelma on erinomainen työkalu Satakunnan ammattikorkeakoulun NGN-laboratorioiden käyttöön sekä opetuksessa, että tutkimustyössä.

Ohjelmaan on saatavilla myös lisäosia, esimerkiksi simulaattori-sovelluksia. Ymmärtääkseni näillä lisäohjelmilla Card Admin voisi tarjota huomattavasti suuremmat mahdollisuudet NGN-laboratorioille, varsinkin opetuskäytössä.

LÄHTEET

1. Mayers, K., Markantonakis, K. Smart Cards, Tokens, Security and Applications. New York: Springer, 2008. 392 p.

2. Rinne, Timo, Älykortit – tekniikka, sovellusalueet ja käyttöönotto. Jyväskylä: satku.fi, 2002. 279 p.

3. Penttinen, Jyrki. Tietoliikennetekniikka 3G ja erityisverkot. WSOY, 2006. 246 p.

4. ETSI verkkosivut [verkkodokumentti]. [Viitattu 31.3.2009.] Saatavissa: http://www.etsi.org/WebSite/AboutETSI/AboutEtsi.aspx

5. Gemalto NV verkkosivut [verkkodokumentti]. [Viitattu 31.3.2009] http://www.gemalto.com/products/card_admin/download/CardAdmin.pdf

6. ETSI TS 121.111 V8.2.0 RELEASE 8 (2008-07), Universal Mobile Telecommunications System (UMTS); USIM and IC card requirements (3GPP TS 21.111 version 8.2.0 Release 8), Sophia Antipolis Cedex : ETSI, 2008. 17 p.

7. ETSI TS 131.102 V8.4.0 (2009-01), Universal Mobile Telecommunications Systems (UMTS); LTE; Characteristics of the Universal Subscriber Indentity Module (USIM) application (3GPP TS 31.102 version 8.4.0 Release 8), Sophia Antipolis Cedex: ETSI, 2009. 207 p.

8. ADN ACCESS Developer Network [Viitattu 10.8.2009]. Saatavissa: http://www.accessdevnet.com/index2.php?option=com_content&do_pdf=1&id=126